REMARKS

Reconsideration and allowance of the subject application are respectfully requested. Applicant thanks the Examiner for total consideration given the present application. Claims 1-5 and 7-11 were pending prior to the Office Action. No claims have been added through this reply. No claims have been canceled through this reply. Therefore, claims 1-5 and 7-11 are pending. Claims 1-2, 4-5, and 7-10 are independent. Applicant respectfully requests reconsideration of the rejected claims in light of the remarks presented herein, and earnestly seeks a timely allowance of all pending claims.

Claim Rejection - 35 U.S.C. § 103(a)

Claims 1-5 and 7-11 stand rejected under 35 U.S.C. § 103(a) as being allegedly unpatentable by Sakai et al. (JP 09-128264 A) in view of Hollander et al. (U.S. Patent 6,301,699). Applicant respectfully traverses this rejection.

For a Section 103 rejection to be proper, a *prima facie* case of obviousness must be established. *See M.P.E.P. 2142.* One requirement to establish a *prima facie* case of obviousness is that the prior art references, when combined, must teach or suggest all claim limitations. *See M.P.E.P. 2142; M.P.E.P. 706.02(j).* Thus, if the cited references fail to teach or suggest one or more elements, then the rejection is improper and must be withdrawn.

Argument: Features of claims 1-2, 4-5, and 7-10 are not taught by cited prior art:

Independent claims 1-2, 4-5, and 7-10 have been amended to include additional limitations. More specifically, claim 1 as amended recites, *inter alia*, "reading one byte of the data; judging whether a branch destination address associated with a branch destination is larger than a branch origin address based only on the one byte of the data read; [and] storing the branch origin address associated with the retrieved instruction code and the branch destination address associated with the branch destination of the instruction code when the branch destination address associated with the branch destination is judged to be larger than the branch origin address."

Therefore, the claimed invention has been amended to include the sequential reading of data to be examined, one byte at a time, and when an address of branch destination (a branch destination address) is larger than an address of the current position (a branch origin address) – namely, in the case of a forward branch – the current position address and the branch destination address are associated with each other and stored.

More specially, in the claimed invention, the analysis is performed in one pass (prior art: a looped analysis) based on the claim requiring the judgment be made with only the current one byte of data read (prior art: more than the current byte of data read – a preceding value and a present value) and storing the branch origin address when the branch destination address is judged to be larger than the branch origin address.

For example, Sakai merely discloses a method for a process of tracing instructions of a micro-program in accordance with an execution path wherein a backward branch is detected – meaning re-execution of an already executed instruction followed by recording of a branch origin address and a branch destination address for the above-mentioned backwards branch. For example, Sakai discloses a rear branch detecting part that compares a preceding value and a present value to detect the occurrence of rear branch. (See Sakai, paragraphs 3 and 12-13.)

While Sakai discloses analyzing the micro-program in accordance with the execution path of the instructions, Sakai fails to disclose sequentially reading data to be examined one byte at a time (*i.e.*, in a top down approach), and then performing analysis in one pass. Accordingly, by the claimed invention performing analysis in one pass in accordance with the data sequences (*i.e.*, based only on the current one byte of the data read), the claimed invention clearly distinguishes over the disclosure of Sakai – Sakai is performing analysis in accordance with the execution path of instruction based on both the preceding value and the present value in a loop architecture.

Also, in Sakai, there is a possibility of accidental occurrence of a backward branch toward a region of absent data or an endless loop because of the premise of examining the micro-program – when random byte sequences are included as sequences to be examined. Therefore, Sakai's analysis in accordance with the execution path of instructions includes a crucial problem – a risk of stopping the analysis processing during the procedure. On the contrary, even if

random byte sequences are included in data, the analysis of the claimed invention does not stack or stop because the claimed invention performs the analysis in one pass in accordance with the data sequences.

Furthermore, Sakai fails to explicitly disclose distinguishing the forward-branch instructions individually – as stated above, Sakai merely performs analysis in accordance with the execution path of instruction based on both the preceding value and the present value. Therefore, Sakai fails to explicitly disclose recording of a branch origin address and a branch destination address relating only to a forward-branch.

While Sakai fails to disclose sequentially reading data to be examined one byte at a time and then performing analysis in one pass, Hollander does not make up for the deficiencies as found in Sakai.

Hollander does disclose a method of recording a branch origin address and a branch destination address, and then, performing analysis based on the recording result. However, Hollander discloses that all branch origin address and a branch destination address should be recorded when data to be examined are divided into basic blocks – then, the division of data into the basic blocks is a premise for analysis of an execution path to an invalid jump and of an execution path to a system call. Therefore, Sakai in view of Hollander still fails to disclose the claimed features of sequentially reading data to be examined one byte at a time and then performing analysis in one pass. Therefore, claims 1-2, 4-5, and 7-10 as amended are submitted to be allowable over Sakai and Hollander for at least this reason.

Further, it is noted that Hollander analyzes a whole input string at least three (3) times based on there being an "END OF CODE" at least three (3) times in the flowcharts of Figures 6-7. Therefore, analysis of multi-paths are necessary and Hollander cannot disclose sequentially reading data to be examined one byte at a time and then performing analysis in one pass.

Furthermore, the reason why judgment as to whether or not a "malicious process" is included can be performed by technology disclosed by Hollander lies in that an input string obtained by hooking a function-call is defined as an object to be examined. However, under the situation in which various contents, for example, data and execution codes, etc. flow, and in which the input string cannot be extracted, the "malicious process" cannot be detected by

applying the method of Hollander. More specially, Hollander fails to disclose how the "malicious process" is judged as such when the object to be examined is a part of the execution code or any of the byte sequences.

Claims 1-2, 4-5, and 7-10 as amended are submitted to be allowable over Sakai and Hollander for at least the above reasons. Dependent claims 3 and 11 are allowable for the reasons set forth above with regards to claims 1-2 at least based on their dependency on claims 1-2.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of claims 1-5 and 7-11 under 35 U.S.C. § 103(a).

Reconsideration and allowance of claims 1-5 and 7-11 are respectfully requested for at least the above reasons.

Conclusion

Therefore, for at least these reasons, all claims are believed to be distinguishable over the combination of Sakai and Hollander, individually or in any combination. It has been shown above that the cited references, individually or in combination, may not be relied upon to show at least the features discussed above. Therefore, claims 1-5 and 7-11 are distinguishable over the cited references.

In view of the above remarks and amendments, it is believed that the pending application is in condition for allowance.

Applicant respectfully requests that the pending application be allowed.

Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Aslan Ettehadieh Reg. No. 62,278 at the telephone number of the undersigned below, to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies to charge payment or credit any overpayment to Deposit Account No. 02-2448 for any additional fees required under 37.C.F.R. §§1.16 or 1.17; particularly, extension of time fees.

Dated: July 9, 2009

Respectfully submitted,

By _____ 48,902
Michael K. Mutter
Registration No.: 29,680
BIRCH, STEWART, KOLASCH & BIRCH, LLP
8110 Gatehouse Road
Suite 100 East
P.O. Box 747
Falls Church, Virginia 22040-0747
(703) 205-8000
Attorney for Applicant